CLAIMS

1. A digital rights management system for controlling the distribution of digital content to player applications, the system comprising:

a verification system to validate the integrity of the player applications;

a trusted content handler to decrypt content and to transmit the decrypted content to the player applications, using an extension mechanism defined by the application, and to enforce usage rights associated with the content; and

a user interface control module to ensure that users of the player applications are not exposed to actions that violate the usage rights;

wherein the digital rights management system operates independently without cooperation from the player applications.

2. A digital rights management system according to Claim 1, wherein the verification system includes an off-line verifier to verify that the player applications have certain properties, and to issue trust certificates to verify that the player applications have said properties.

3. A digital rights management system according to Claim 2, wherein the verification system further includes a verifying launcher for verifying that a particular player application is certified as a trusted application before digital content is transmitted to said particular player application.

4. A digital rights management system according to Claim 1, wherein the player applications request protected content, and the trusted content handler includes an authenticator to verify that a player application that

5   requests p●ected content has been au●rized by the

6   verificatioñ system to access the requested, protected

7   content.

1   5. A digital rights management system according to Claim

2   1, wherein a user interface control module traps user

3   interface related messages generated as a result of user

4   interactions with player applications, blocks messages

5   that lead to usage rights violations, and passes through

6   other messages to the player applications.

1   6.   A digital rights management method for controlling

2   the distribution of digital content to player

3   applications, the method comprising the steps:

4   providing a verification system to validate the

5   integrity of the player applications;

6   using a trusted content handler to decrypt content

7   and to transmit the decrypted content to the player

8   applications, using an extension mechanism defined by the

9   applications, and to enforce usage rights associated with

10   the content; and

11   providing a user interface control module to ensure

12   that users of the player applications are not exposed to

13   actions that violate the usage rights;

14   wherein the digital rights management system

15   operates independently without cooperation from the

16   player applications.

1   7.   A method according to Claim 6, wherein the step of

2   providing a verification system includes the step of

3   providing an off-line verifier to verify that the player

4   applications have certain properties, and to issue trust

5   certificates to verify that the player applications have

6   said properties.

1   8.   A method according to Claim 7, wherein the step of
2   providing a verification system further includes the step
3   of providing a verifying launcher for verifying that a
4   particular player application is certified as a trusted
5   application before digital content is transmitted to said
6   particular player application.

1   9.   A method according to Claim 6, wherein the player
2   applications request protected content, and the step of
3   using the trusted content handler includes the step of
4   using an authenticator to verify that a player application
5   that requests protected content has been authorized by the
6   verification system to access the requested, protected
7   content.

1   10.   A program storage device readable by machine,
2   tangibly embodying a program of instructions executable by
3   the machine to perform method for controlling the
4   distribution of digital content to player applications,
5   the method steps comprising:
6   using a verification system to validate the integrity
7   of the player applications;
8   using a trusted content handler to decrypt content
9   and to transmit the decrypted content to the player
10 applications, using an extension mechanism defined by the
11 applications, and to enforce usage rights associated with
12 the content; and
13   using a user interface control module to ensure that
14 users of the player applications are not exposed to
15 actions that violate the usage rights;
16   wherein said method operates independently without
17 cooperation from the player applications.

1   11. A program storage device according to Claim 10,
2   wherein the step of using the verification system includes

3   the step of using an off-line verifier to verify that the
4   player applications have certain properties, and to issue
5   trust certificates to verify that the player applications
6   have said properties.

1   12. A program storage device according to Claim 11,
2   wherein the step of using the verification system further
3   includes the step of using a verifying launcher for
4   verifying that a particular player application is
5   certified as a trusted application before digital content
6   is transmitted to said particular player application.

1   13. A program storage device according to Claim 10,
2   wherein the player applications request protected content,
3   and the step of using the trusted content handler includes
4   the step of using an authenticator to verify that a player
5   application that requests protected content has been
6   authorized by the verification system to access the
7   requested, protected content.

1   14. A code identity and integrity verification system,
2   comprising:
3   a certificate generator for receiving applications,
4   for determining if the applications exhibit a predefined
5   property, and for issuing a trust certificate for each of
6   the applications that exhibits the predefined property;
7   a certificate repository for receiving and storing
8   trust certificates issued by the certificate generator;
9   a code verifier for verifying that a particular
10   player application is certified as a trusted application
11   before digital content is transmitted to said particular
12   player application; and
13   an authenticator for receiving requests, using an
14   extension mechanism defined by the applications, to verify
15   that a player application that requests protected content

16 has been a●orized by the verificatio●ystem to access
17 the requested, protected content.

1   15. A code identify and integrity verification system
2   according to Claim 14, wherein the code verifier is
3   responsible for launching the player application and
4   verifying the identity and integrity of the code using the
5   information in the trust certificate before launching the
6   application; the launch procedure returning process
7   identification information, which the code verifier
8   records internally; the authenticator communicating the
9   same or other process identification information
10 concerning its own process, which it obtains from system
11 service calls, to the code verifier at the time the
12 application requests content from the authenticator; the
13 code verifier matching this process identification
14 information against the process identification information
15 it recorded; the code verifier returning a code indicating
16 whether the process was verified or not.

1   16. A code identity and integrity verification system
2   according to Claim 14, wherein the code verifier receives
3   from the authenticator process identification information
4   at the time the player application calls the
5   authenticator; the code verifier querying the operating
6   system with the process identification information or the
7   file names of all modules loaded for that process; the
8   code verifier using the information in the trust
9   certificate to verify the identity and integrity of the
10 code modules; returning a code indicating whether the
11 process was verified or not.

1   17. A code identity and integrity verification system
2   according to Claim 14, wherein the trust certificate
3   includes:

4   a pro⬤am identifier identifying ⬤d one of the
5   applications;
6   a property name identifying an attribute certified by
7   the trust certificate;
8   a code digest of the one application;
9   a digital signature containing a secret key of the
10   application certifier; and
11   a certifier identification containing a public key of
12   the application certifier.

1   18. A method for verifying the identity and integrity of
2   code, comprising the steps:
3   using a certificate generator for receiving
4   applications, for determining if the applications exhibit
5   a predefined property, and for issuing a trust certificate
6   for each of the applications that exhibits the predefined
7   property;
8   receiving and storing in a certificate repository
9   trust certificates issued by the certificate generator;
10   using a code verifier for verifying that a particular
11   player application is certified as a trusted application
12   before digital content is transmitted to said particular
13   player application; and
14   using an authenticator for receiving requests, using
15   an extension mechanism defined by the application, to
16   verify that a player application that requests protected
17   content has been authorized by the verification system to
18   access the requested, protected content.

1   19. A method according to Claim 16, wherein the trust
2   certificate includes:
3   a program identifier identifying said one of the
4   applications;
5   a property name identifying an attribute certified by
6   the trust certificate;

7   a code digest of the one application;

8   a digital signature containing a secret key of the

9 application certifier; and

10   a certifier identification containing a public key of

11 the application certifier.

1 20. A program storage device readable by machine, tangibly

2 embodying a program of instructions executable by the

3 machine to perform method steps for verifying, out of

4 process, the identity of code, said method steps

5 comprising:

6   using a certificate generator for receiving

7 applications, for determining if the applications exhibit

8 a predefined property, and for issuing a trust certificate

9 for each of the applications that exhibits the predefined

10 property;

11   receiving and storing in a certificate repository

12 trust certificates issued by the certificate generator;

13   using a code verifier for verifying that a particular

14 player application is certified as a trusted application

15 before digital content is transmitted to said particular

16 player application; and

17   using an authenticator for receiving requests, using

18 an extension mechanism defined by the application, to

19 verify that a player application that requests protected

20 content has been authorized by the verification system to

21 access the requested, protected content.

1 21. A program storage device according to Claim 20,

2 wherein the trust certificate includes:

3   a program identifier identifying said one of the

4 applications;

5   a property name identifying an attribute certified by

6 the trust certificate;

7   a code digest of the one application;

8   a digital signature containing a secret key of the
9 application certifier; and
10   a certifier identification containing a public key of
11 the application certifier.